

AMENDMENTS

In the Claims

1. (currently amended) A system for providing a secure document, the system including: a
5 computer network including a computer and an RFID transponder, the computer having a
database, and the database containing a first authorization key and at least one additional
authorization key; the secure document, the secure document including an integrated RFID
circuit coupled with a flexible substrate; the flexible substrate having a surface, the surface
visibly presenting an information; the integrated RFID circuit coupled with the substrate, and the
10 integrated RFID circuit having a durable memory, a controller, and a data security circuit; the
durable memory including an information storage sector and a protected sector, the information
storage sector having a record of at least a portion of the information, and the protected sector
having at least one datum not recorded within the information of the flexible substrate; the
controller coupled with the durable memory and the data security circuit, and the controller for
15 enabling access to the durable memory by the RFID transponder as authorized by the data
security circuit; and the data security circuit for denying authority to the controller to execute
instructions received in a message, where the message is not formatted at least partially in
mathematical relationship to the first authorization key, wherein different authorization keys are
provided to different parties to form a hierarchy of access to various portions of the information
20 stored within the durable memory.

2. (original) The system of claim 1, the system further comprising a printer, the printer communicatively coupled with the computer and the printer for adding visible information to the surface of the flexible substrate.

5 3. (original) The system of claim 1, wherein the first authorization key is at least partially computed on the basis of biometric data.

4. (original) The system of claim 1, wherein the message is a revocation of a validity state of the secure document.

10

5. (original) The system of claim 1, wherein the secure document is a payroll check.

6. (original) The system of claim 1, wherein the secure document is a certified check.

15 7. (original) The system of claim 1, wherein the secure document is a cashier's check.

8. (original) The system of claim 1, wherein the secure document is a note of currency issued by a governmental authority.

20 9. (currently amended) The system of claim 1, the system further comprising: a plurality of authorization keys, the plurality of authorization keys stored within the durable memory and the plurality of authorization keys stored within at least one data storage device communicatively

coupled with the computer network; and the plurality of authorization keys arranged within a hierarchy, wherein the data security circuit authorizes the controller to execute an instruction received within a message, ~~wherein the message is at least partially formatted in mathematical relationship to at least one of the plurality of authorization keys~~, and the data security circuit
5 limits a scope of execution of the instruction in light of the position of the at least one of the plurality of authorization keys within the hierarchy, wherein different authorization keys are provided to different parties to form a hierarchy of access to various sectors of protected information.

10 10. (currently amended) A secure document system comprising: a device comprising a flexible substrate coupled with an integrated circuit; means for printing information onto a flexible substrate; the integrated circuit including a durable memory storing digital data; and the durable memory further storing at least ~~[[one]]~~ two authorization keys, wherein at least one of the at least two authorization keys are ~~[[key is]]~~ written into the durable memory at
15 approximately the time that visible information is added to the flexible substrate, the integrated circuit including a circuit that allows external access to certain portions or the stored digital data only to interrogators ~~[[with]]~~ communicating the requisite authorization key or keys, wherein different authorization keys are provided to different parties to form a hierarchy of access to various sectors of protected information.

20

11. (original) The system of claim 10, wherein the printer further comprises an RFID transmitter, the transmitter using the authorization key or keys to gain access to at least one section of the durable memory.

5 12. (original) The system of claim 10, wherein the digital data includes a unique identification number.

13. (original) The system of claim 10, wherein the digital data includes a portion of the information that is printed on the flexible substrate.

10 14. (original) The system of claim 10, wherein the device is a form of currency document or other monetary instrument.

15 15. (original) The system of claim 10, wherein the device is a personal, certified, payroll, or other form of check.

16. (original) The device of claim 10, wherein the device is an airline ticket.

17. (original) The system of claim 10, wherein the durable memory also includes other
20 information about the ticket such as destination, a unique identity number, flight number, and cost of the ticket.

18. (original) The system of claim 10, wherein the device is a coupon.

19. (original) The system of claim 18, where the durable memory also includes additional information about the coupon such as the manufacturer of the coupon product, a unique identity number, or the redemption value of the coupon.

20. (original) The system of claim 1, wherein the first authorization key that includes a checksum, the checksum computed upon the basis of at least a portion of the information printed on said document.

21. (original) The system of claim 20, wherein the checksum is computed upon the basis of at least one datum stored within the integrated RFID circuit and at least a portion of the information printed on the secure document.

22. (original) The system of claim 2, wherein the secure document is a personal check

23. (original) The system of claim 2, wherein the secure document is an airline ticket.

24. (original) The system of claim 2, wherein the durable memory stores information related to a travel destination.

25. (original) The system of claim 2, wherein the durable memory stores information related to an airline flight.

26. (original) The system of claim 2, wherein the durable memory stores information related to
5 a price of an airline ticket.

27. (original) The system of claim 2, wherein the durable memory stores information related to a coupon.

10 28. (original) The system of claim 27, wherein the durable memory stores information related to a manufacturer.

29. (original) The system of claim 27, wherein the durable memory stores information related to a product identifier.

15 30. (original) The system of claim 27, wherein the durable memory stores information related to a redemption value of the coupon.

31. (cancelled) A system for providing a secure document, the system including: a
20 computer network including a computer and an RFID transponder, the computer having a database, and the database containing at least two different authorization keys; the secure document, the secure document including an integrated RFID circuit coupled with a flexible

substrate; the flexible substrate having a surface, the surface visibly presenting an information; the integrated RFID circuit coupled with the substrate, and the integrated RFID circuit having a durable memory, a controller and a data security circuit; the durable memory including at least two protected sectors, the each protected sector containing information not contained any of the other sectors; and the controller coupled with the durable memory and the data security circuit, and the controller for enabling access to the durable memory by the RFID transponder only when authorized by the data security circuit in response to the presentation to the data security circuit of data and instructions that have been encoded with the correct authorization keys.

32. (currently amended) A system for providing a secure document, [[The]] the system [[of claim 31]] including: a computer network including a computer and an RFID transponder, the computer having a database, and the database containing at least two different authorization keys; a secure document, the secure document including an integrated RFID circuit coupled with a flexible substrate; the flexible substrate having a surface, the surface visibly presenting an information; the integrated RFID circuit coupled with the substrate, and the integrated RFID circuit having a durable memory, a controller and a data security circuit; the durable memory including at least two protected sectors, the each protected sector containing information not contained in any of the other sectors; and the controller coupled with the durable memory and the data security circuit, and the controller for enabling access to the durable memory by the RFID transponder only when authorized by the data security circuit in response to the presentation to the data security circuit of data and instructions that have been encoded with one of a plurality

authorization keys, wherein different authorization keys are provided to different parties to
[[form]] enable a hierarchy of access to various sectors of protected information.

33. (currently amended) A method for detecting the use counterfeit currency wherein
5 financial instruments are fabricated with embedded electronic devices containing multiple
sectors of hidden information protected by multiple authorization keys and initial authentication
is achieved using certain keys, and wherein back-up authentication is achieved by using other
authentication keys not available to the parties doing the initial authentication, wherein different
authorization keys are provided to different parties to form a hierarchy of access to various
10 sectors of protected information.

34. (currently amended) The system of claim 1, wherein the durable memory further
comprises [[a record of an EPC]] an Electronic Product Code.

15 35. (original) The system of claim 1, wherein the durable memory further comprises a record of
an Electronic Product Code.

36. (new) The method of Claim 32, wherein the information stored in the durable memory
comprises a biometric information and the biometric information is authenticated via the
20 computer network by comparison of the biometric information with remote information stored in
a remote database of the computer network.